ZEROFOX

DESCRIPCIÓN

Plataforma de ciberseguridad externa ZeroFox

Protección más allá del perímetro

Índice

DESCRIPCIÓN DEL PROBLEMA

En el primer mundo digital actual, casi todas las empresas utilizan plataformas públicas, ya sean redes sociales, sitios web, aplicaciones móviles o herramientas de colaboración, para conectarse con sus clientes. Sin embargo, estas mismas plataformas ayudan a los atacantes a sembrar el caos en nuestras vidas digitales, creando una inmensa superficie de ataque pública. Los ciberdelincuentes tienen acceso tanto a clientes como a otros miembros de la empresa e intentarán suplantar la identidad de marcas y ejecutivos, falsificar sitios protegidos, desviar las ganancias del negocio, robar datos confidenciales, estafar a los empleados y destruir la confianza del cliente. Desafortunadamente, muchas de las plataformas digitales actuales carecen de funciones de administración, monitoreo y protección más allá de los perímetros de seguridad tradicionales.

Ante esta falta de visibilidad y control, con escasez de personal cualificado y con sistemas de seguridad anticuados, las empresas tienen problemas para identificar y neutralizar los riesgos digitales externos, y para protegerse en esta vasta superficie de ataque pública.

DESCRIPCIÓN DE LA SOLUCIÓN

ZeroFox, líder mundial en protección e inteligencia sobre amenazas externas, proporciona una protección integral y una orquestación escalable de inteligencia automática y humana con el objetivo de garantizar la seguridad de la superficie de ataque pública de las organizaciones, protegiendo a los empleados y los clientes frente a las amenazas digitales externas. La plataforma ZeroFox monitorea continuamente las plataformas digitales disponibles para el público, con el fin de descubrir ciberactividad maliciosa y amenazas ocultas dirigidas contra su organización o sus clientes. Además, se coordina de manera proactiva con los proveedores de red y de hosting para neutralizar las amenazas y desmantelar la infraestructura completa del atacante, antes de que pueda provocar daños.

Mediante el empleo de diversas fuentes de datos y análisis basados en inteligencia artificial, la plataforma ZeroFox identifica y evita las amenazas dirigidas, que abundan en las plataformas públicas. ZeroFox monitorea continuamente para localizar amenazas emergentes, alerta inmediatamente a los equipos de seguridad y las autoridades cuando se inicia el ataque, y aplica automáticamente rápidas medidas de corrección que incluyen desde la moderación del contenido ofensivo hasta la desarticulación total de la infraestructura de ataque del adversario.

Además, los investigadores de amenazas de ZeroFox filtran los hallazgos y proporcionan un flujo continuo de informes relevantes, con contexto y análisis, para satisfacer sus requisitos de inteligencia prioritarios. Si se produce un compromiso, nuestros agentes de la web oscura facilitan el contacto directo con el atacante para investigar las amenazas emergentes, recuperar los recursos y negociar las condiciones de un acuerdo.

La plataforma ZeroFox

La plataforma ZeroFox es una solución de protección ante riesgos digitales y de inteligencia global sobre amenazas, fácil de desplegar, siempre activa y basada en la nube, que ofrece a las organizaciones visibilidad y protección integrales en la web de superficie, la web profunda y la web oscura.

La plataforma ZeroFox ofrece detección y neutralización automáticas de amenazas procedentes de una amplia variedad de fuentes de datos, en continua evolución. ZeroFox identifica los riesgos y amenazas tanto para las empresas como para los empleados. Mediante una combinación de tecnologías basadas en inteligencia artificial y analistas de amenazas encargados de identificar los riesgos y filtrar las alertas, la plataforma ZeroFox identifica y aplica automáticamente las acciones necesarias para resolver problemas de cuentas fraudulentas, ataques de phishing/smishing, estafas a clientes, vulneración de datos de identificación personal y credenciales comprometidas, entre otros.

La plataforma ZeroFox ofrece

Visibilidad en todos los canales

Proteja a su empresa frente a los riesgos dinámicos de la seguridad en la más amplia variedad de plataformas de la industria, incluidas la web de superficie, la web profunda y la web oscura, las redes sociales, las apps para móviles, los repositorios de código compartido, el correo electrónico y las plataformas de colaboración, entre otras. Tenga la tranquilidad de saber que si surge una nueva amenaza, usted la verá primero.

Descubrimiento de amenazas con inteligencia artificial

Gracias al empleo a una escala sin precedentes de técnicas de aprendizaje automático y análisis basado en inteligencia artificial, la plataforma ZeroFox identifica automáticamente en objetos, imágenes y video las amenazas ocultas que escapan a la detección, y evita ataques de phishing dirigido, compromisos de credenciales, robos de datos, suplantaciones de identidad, secuestros de marcas, amenazas contra directivos y ubicaciones, etc.

Amplia inteligencia de amenazas y búsqueda exhaustiva de amenazas

Enriquezca los programas de seguridad tradicionales con inteligencia especialmente centrada en las vulnerabilidades de las redes sociales y los medios digitales, y en las amenazas en la web de superficie, profunda y oscura. ZeroFox ofrece búsqueda de amenazas en la plataforma, mediante un inmenso lago con petabytes de datos de inteligencia filtrada, junto con un equipo de investigadores de amenazas, analistas y agentes de la web oscura, que se suman a su equipo para dar una respuesta ante la escala y el nivel de sofisticación de las amenazas externas.

Neutralización automática y disrupción total del adversario

ZeroFox proporciona servicios de desmantelamiento integrales como ocultar, bloquear y eliminar el contenido malicioso u ofensivo, eliminar las cuentas y sitios falsos, y aplicar los términos de servicio, para afrontar directamente las amenazas. ZeroFox va un paso más allá y bloquea a los atacantes inhabilitando su infraestructura en asociación con nuestra red de disrupción global (Global Disruption Network, GDN).

PROTECCIÓN de sus recursos fuera del perímetro › **PREDICCIÓN** de amenazas emergentes con inteligencia global › **DISRUPCIÓN** de ataques y desmantelamiento de la infraestructura del adversario

PROTECCIÓN FRENTE A RIESGOS DIGITALES

Protección de los recursos fuera del perímetro

La protección solo funciona si es específica para su caso. Debe centrar sus esfuerzos de protección en los riesgos y amenazas a las que se enfrenta cada día. ZeroFox empieza por definir los recursos más importantes para su organización: marcas, empleados, directivos y personas VIP, productos, ubicaciones y páginas corporativas.

Estos recursos se componen de una variedad de "objetos" diferentes, como perfiles, nombres, palabras clave, imágenes, dominios, hashtags, etc. Esto determina cómo y de dónde recopila datos ZeroFox, garantizando que lo que obtiene sean solo datos relevantes para su organización. Durante el proceso de incorporación, nuestro equipo de especialistas en lanzamiento le ayudará a configurar y personalizar correctamente la plataforma, según sus especificaciones.

Protección de la marca

Monitoreo para detectar amenazas contra marcas, submarcas y organizaciones en todas las fuentes de datos de la web de superficie, profunda y oscura. Esto incluye la suplantación de la marca, menciones o evidencias de la vulneración de recursos o datos de una empresa, como fugas de datos, credenciales comprometidas, robos de tarjetas de crédito y otros datos de identificación personal o de propiedad intelectual.

Protección avanzada contra phishing e uso ilícito de dominios

ZeroFox monitorea y procesa continuamente cientos de millones de sitios web, e identifica vulneraciones en las que se emplean términos relativos a su organización, en registros y URL de phishing conocidas y nuevas, con independencia de si están alojadas en dominios o subdominios. Además, ZeroFox supervisa para descubrir código robado de sitios web y fuentes de datos de phishing en el conjunto del contenido alojado, y le alerta si su logotipo, términos de la marca o imágenes faciales detectadas se han incluido como parte de contenido de phishing alojado.

Protección de directivos

Protección de las personas VIP frente a las usurpaciones de cuentas, las suplantaciones de identidad, las fugas de datos confidenciales, el doxxing, el compromiso de credenciales, así como las ciberamenazas y las amenazas físicas. La protección de directivos incluye a los ejecutivos de alto nivel, los empleados y las personas VIP, así como las cuentas de redes sociales individuales asociadas.

Protección de productos y contra falsificaciones

Protección de los entregables físicos principales, el software, los trabajos digitales, el servicio y la propiedad intelectual de su marca. ZeroFox ofrece protección contra uso ilícito de marcas, fraude, piratería y falsificación de productos.

Protección de la superficie de ataque y las vulnerabilidades

Avisos de vulnerabilidades del sistema para poder prevenir y mitigar de forma proactiva las violaciones de seguridad, las fugas de datos, el compromiso de credenciales y otras amenazas que ponen a la organización en riesgo. Se pueden descubrir los recursos de TI y de la nube desprotegidos, como los externos que están "fuera del firewall" y los analizables (servidores, hosts web, contenedores basados en la nube, etc.) y comprobar si hay vulnerabilidades, como contraseñas predeterminadas, puertos abiertos, errores de configuración, certificados caducados u otros parámetros no seguros.

Seguridad de directivos y personas VIP

Monitoreo de los canales digitales y los eventos del mundo real que ponen en peligro la seguridad del personal y, en particular, la de los individuos muy prominentes. Proporcione un servicio de protección VIP especializado en evaluaciones de amenazas, monitoreo 24x7, alertas y escalada, investigación de amenazas para la seguridad física o cobertura de los familiares directos, entre otros temas.

Protección de cuentas de redes sociales corporativas

Proporcione control y seguridad para las cuentas y páginas de redes sociales de la empresa u organización. Evite los intentos de hackeo y secuestro de cuentas, y faciilite la moderación del contenido en línea para eliminar los comentarios ofensivos o inapropiados.

Monitoreo y protección de la web oscura y profunda

Supervise continuamente los nuevos grupos de datos para detectar nueva información en la web oscura y proporcionar una amplia cobertura de los canales digitales no indexados. Obtenga visibilidad de las credenciales comprometidas, así como de cualquier otra información confidencial, descubra fugas de datos sensibles, y consiga información de las tácticas empleadas por los ciberdelincuentes y la planificación de los ataques.

Inteligencia de seguridad física (PSI)

Infórmese casi en tiempo real con avisos de alerta instantáneos sobre incidentes globales que amenazan la seguridad física de sus directivos, los miembros de sus equipos, sus instalaciones, etc. El equipo del centro de operaciones (SOC) de seguridad física 24/7 de ZeroFox investiga y valida continuamente los eventos que implican un riesgo o alteración inmediata de la seguridad pública (como los tiroteos, protestas, desastres naturales, avisos sobre seguridad si se va a viajar, etc.), procedentes de fuentes muy diversas de inteligencia humana (HUMINT) y de inteligencia de fuentes abiertas (OSINT) en la web de superficie, profunda y oscura.

Protección contra fraudes en el correo electrónico y phishing

Amplíe la protección de su organización y detecte vulneraciones de marca que aprovechan información existente, como los informes de fallos de DMARC y mensajes "abuse@....." reenviados. Esto funciona de forma conjunta con los gateways antispam, antivirus y de filtrado del correo destinados a proteger a los usuarios y el contenido de los mensajes.

Protección de ubicaciones y eventos

Protección de los recursos locales, como sedes, instalaciones de fabricación, almacenes y centros de distribución, oficinas y tiendas, puntos de origen y destinos temporales, contra comentarios relacionados con viajes, y amenazas físicas y relativas a la ubicación. Además, se obtiene información de la situación y avisos tempranos acerca de la planificación de ataques, incidentes de seguridad pública o amenazas cuando sean cercanos a sus ubicaciones y eventos.

Protección frente a Business Email Compromise (BEC)

Análisis de las bandejas de entrada para identificar mensajes maliciosos relacionados con ataques BEC (también denominados fraudes del CEO), marcar dichos mensajes con banners de aviso e impedir que los dominios maliciosos alojen direcciones de correo electrónico del atacante, con el fin de garantizar la protección de sus empleados y clientes.

Protección de los empleados remotos

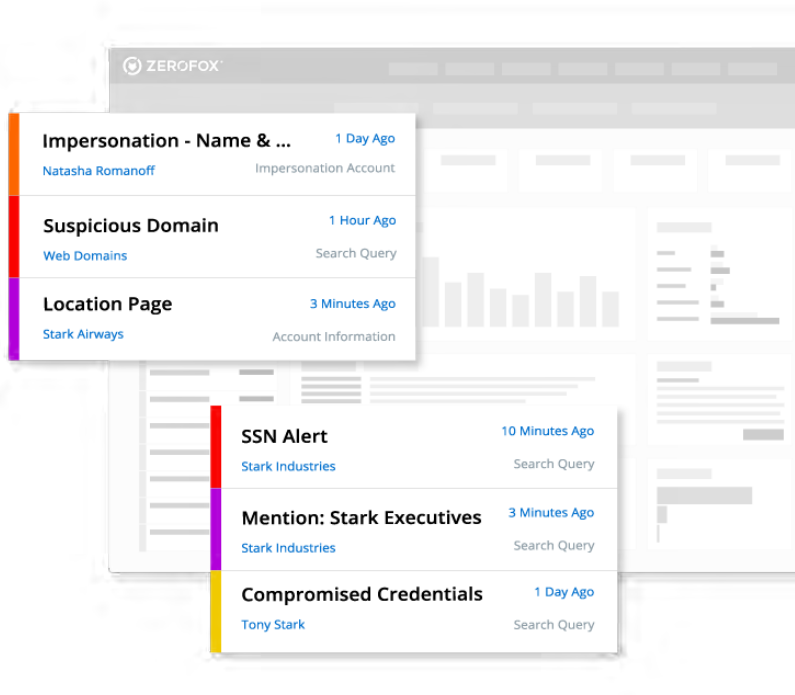
Supervisión de chats y listas de asistentes para detectar signos de actividad maliciosa o inapropiada con el fin de garantizar la seguridad en las videoconferencias para empleados, clientes y partners. ZeroFox for Slack protege a sus equipos de colaboración internos y externos, identificando y eliminando de los canales de Slack el contenido malicioso, inadecuado o confidencial.

Protección de la cadena de suministro

ZeroFox llega aún más lejos y protege el ecosistema completo de su cadena de suministro. Supervisa, alerta y evita los riesgos, las amenazas y los ataques contra terceros que afectan a sus recursos de la cadena de suministro, como los dominios, marcas y directivos de los partners.

Amenazas sociales y digitales externas

- Credenciales comprometidas
- Robo de identidad y de información de identificación personal
- Uso inapropiado de contenido
- Amenazas emergentes
- Planificación y conversaciones sobre ataques furtivos
- Usurpación de cuentas
- Pérdida de datos
- Incumplimiento de normativas
- Kits de phishing
- Typosquatting de dominios
- Suplantación de identidad de directivos/ejecutivos
- Fraude, piratería y estafas
- Suplantación de marca
- Amenazas violentas
- Aprovechamiento de vulnerabilidades externas
- Amenazas físicas
- Amenazas internas
- Amenazas relacionadas con viajes
- Cuentas y dominios falsificados
- Phishing/smishing/vishing, malware y enlaces maliciosos



CASOS DE USO

ZeroFox proporciona a los equipos de seguridad de la información, seguridad de la empresa y protección de marca la visibilidad, inteligencia y respuesta automatizada que necesitan para proteger contra:

Phishing y malware dirigidos

Los ciberdelincuentes usan URL abreviadas u ocultas como principal mecanismo de distribución del ataque, y aprovechan las redes sociales para sortear las medidas de seguridad y atacar tanto a empleados como a clientes. Otras tácticas de phishing de dominios son la ciberocupación y el typosquatting, así como el empleo de homoglinfos. Identifique y evite las URL maliciosas en su entorno de redes sociales.

Ransomware

Actúe cuando reciba los primeros indicios de ataques de ransomware, desde los primeros avisos de presencia de credenciales en la web oscura hasta el contacto directo con los ciberdelincuentes en sitios clandestinos. Además, puede trabajar con un intermediario para negociar la recuperación de los recursos o realizar pagos en criptomoneda, cuando sea necesario.

Cuentas comprometidas

Las cuentas de redes sociales son fuentes de información corporativa de confianza, sin embargo, a diferencia de los sitios web, carecen de seguridad y protección, a excepción de una contraseña básica. Esté atento para detectar comportamientos o comentarios sospechosos y bloquee todo el contenido saliente desde una cuenta comprometida.

Amenazas contra directivos y empresas

Los directivos y los recursos corporativos están expuestos a riesgos en la web oscura e incluso en las redes sociales, como el doxxing, la pérdida de información de identificación personal, las amenazas físicas y la exposición de datos sobre viajes. Monitoree las cuentas de directivos, ejecutivos y empleados y vigile el mundo digital para detectar actividades maliciosas, amenazas o la exposición de contenido confidencial.

Suplantación de la marca y las cuentas de directivos

Las cuentas fraudulentas y falsas sacan partido de la confianza implícita que se otorga en las redes sociales, el correo electrónico y los sitios web legítimos, para lanzar ataques de phishing, llevar a cabo estafas y causar daños a las marcas. Identifique y elimine las cuentas, direcciones de correo electrónico y dominios que suplantan la identidad de su marca o su personal.

Credenciales comprometidas y fuga de información

Una vez que los atacantes roban las credenciales de los empleados y la información corporativa, publicitan, venden y distribuyen estos datos confidenciales en la web profunda y oscura. ZeroFox analiza estos canales para identificar dónde se han divulgado estos datos u otra propiedad intelectual sensible de la empresa.

Fraude y timos de clientes

Ya sea a través de timos financieros, estafas relacionadas con la facturación u ofertas falsas, las redes sociales y las plataformas digitales ponen en peligro la reputación de sus clientes y su marca. Identifique la actividad maliciosa y limite los costos que acarrea la neutralización, la asistencia al cliente y la pérdida de oportunidades de negocio.

Planificación y conversaciones sobre ataques furtivos

Los ciberdelincuentes suelen aprovechar canales encubiertos y sitios no indexados en la web profunda y oscura para planificar, coordinar y hablar de los próximos ataques. Vaya al grano y descubra esa conversación sobre ataques que menciona precisamente sus marcas, directivos y recursos protegidos, y detecte automáticamente las comunicaciones encubiertas que delatan una intención u opinión malintencionada.

Piratería y falsificaciones

El contenido falso o robado que se comparte en marketplaces o mercados de la web oscura y se promociona en redes sociales puede afectar seriamente a sus ingresos. Identifique automáticamente el contenido privativo que circula por las redes sociales, tanto si se ha publicado intencionadamente como si no.

Riesgos de vulnerabilidades externas

Los ciberdelincuentes suelen intentar aprovechar vulnerabilidades externas y recursos de la nube desprotegidos, situados fuera del firewall. De esa forma, abren la puerta a riesgos de violaciones de seguridad, fugas de datos, ataques de phishing, etc. Identifique y compruebe si hay recursos de TI o de la nube desprotegidos.

Conocimiento de la situación del entorno físico y virtual

Los adversarios, ya sean físicos o digitales, suelen comunicar sus intenciones por Internet. Monitoree para localizar términos y frases clave específicas de su organización que le alerten de conversaciones maliciosas sobre su empresa o publicaciones dentro de una zona geográfica concreta.

Riesgos para la seguridad física globales

Los incidentes y eventos del mundo real a menudo ponen en riesgo la seguridad física de directivos clave, sus ubicaciones y sus empresas. Manténgase al tanto de los incidentes o alteraciones de la seguridad pública en su zona y reciba alertas de eventos que puedan poner en riesgo la seguridad de sus centros de trabajo y su personal.

Riesgos en las páginas corporativas y cumplimiento de normativas

Es habitual que haya trolls, remitentes de spam, competidores, ciberdelincuentes y clientes descontentos que publiquen contenido malicioso, ofensivo o sensible en las páginas de la empresa. Bloquee, oculte o elimine inmediatamente el contenido no deseado, como calumnias, números de tarjetas de crédito, estafas y enlaces de phishing.

Amenazas internas

El riesgo de amenazas internas incluye desde empleados descontentos que huyen con datos sensibles hasta personal que publica contenido no autorizado en redes sociales o en herramientas de colaboración, así como amenazas tanto físicas como digitales. Identifique la actividad maliciosa específica para su organización, tanto si es externa como interna.

INTELIGENCIA DE AMENAZAS GLOBAL

Predicción de amenazas emergentes

ZeroFox proporciona una exhaustiva inteligencia de amenazas sobre adversarios modernos, ataques externos y sus indicadores digitales, que los proveedores de inteligencia de amenazas digital no ofrecen. La combinación de la plataforma ZeroFox basada en inteligencia artificial, un enorme lago de datos de inteligencia de amenazas y amplias funciones de inteligencia humana de la web oscura ofrece protección automatizada e información para organizaciones de todos los tamaños. Transforme datos brutos en inteligencia práctica, con la posibilidad de que le sirva para incrementar la eficiencia y la eficacia de los equipos de seguridad.

TIPOS DE INTELIGENCIA GLOBAL

Inteligencia de la web oscura

Acceso a datos de la web oscura y la web profunda para identificar la presencia de credenciales robadas o expuestas, información de identificación personal, direcciones IP, etc., antes de que se aprovechen en ataques dirigidos contra su organización.

Inteligencia de vulnerabilidades

Control de las últimas vulnerabilidades publicadas por otros proveedores. Supervisión de las vulnerabilidades y los exploits que tanto las comunidades de investigadores de seguridad como de ciberdelincuentes consideran prioritarios.

Inteligencia sobre la marca

Identificación de dominios fraudulentos, suplantación de identidad de directivos, phishing y otros riesgos en la superficie de ataque pública que ponen su marca en peligro.

Inteligencia sobre seguridad física

Monitoreo de eventos o políticas que afectan a zonas geográficas de actuación concretas o bien a directivos específicos. Controle las técnicas, tácticas y procedimientos (TTP) que afectan a su estado de ciberseguridad y seguridad física.

Inteligencia sobre fraudes

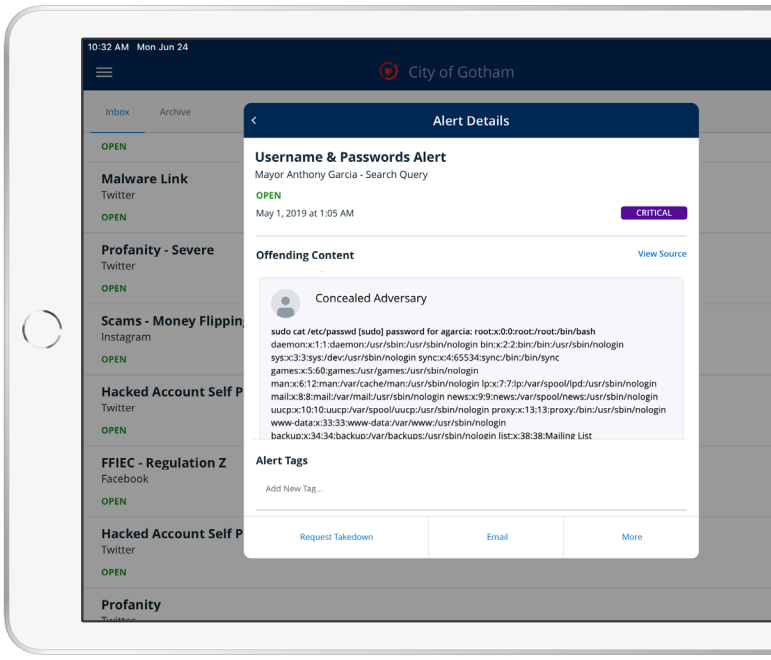
Información sobre conjuntos de datos, sitios web, herramientas, especialistas en fraude y las técnicas, tácticas y procedimientos (TTP) y métodos de ingeniería social que emplean, con el objetivo de destruir su empresa y perjudicar a sus clientes.

Inteligencia de terceros

Control del riesgo potencial para proveedores y empresas de partners pertenecientes a su cadena de suministro en todo el espectro de inteligencia de amenazas.

Inteligencia de la infraestructura de Internet

Distinción entre proveedores legítimos y sospechosos de dominios e infraestructuras de hosting/VPS. Descubra los exploits y TTP actuales de la infraestructura, los hosts sospechosos, y las direcciones IP y dominios utilizados en los ataques.



Inteligencia geopolítica

Una visión de los riesgos a los que se enfrenta su organización o las operaciones que realiza en una región concreta del mundo, ya sea en el ámbito político, cultural, legal, sanitario u otros.

Inteligencia de malware y ransomware

Localización rápida del malware, los atacantes y las TTP que utilizan para conseguir acceder, escalar, filtrar información y pedir un rescate en su organización.

Inteligencia estratégica

Control de los eventos geopolíticos, y los indicadores sociales, sanitarios y económicos para poder tomar decisiones fundamentadas y duraderas.

INFORMES Y ENTREGABLES DE INTELIGENCIA GLOBAL

Últimas noticias

Los investigadores de amenazas de ZeroFox filtran y contextualizan las últimas noticias relevantes, y se las hacen llegar a los usuarios mediante la plataforma ZeroFox, así como a través del correo electrónico en el informe de amenazas diarias de ZeroFox.

Análisis de amenazas personalizado

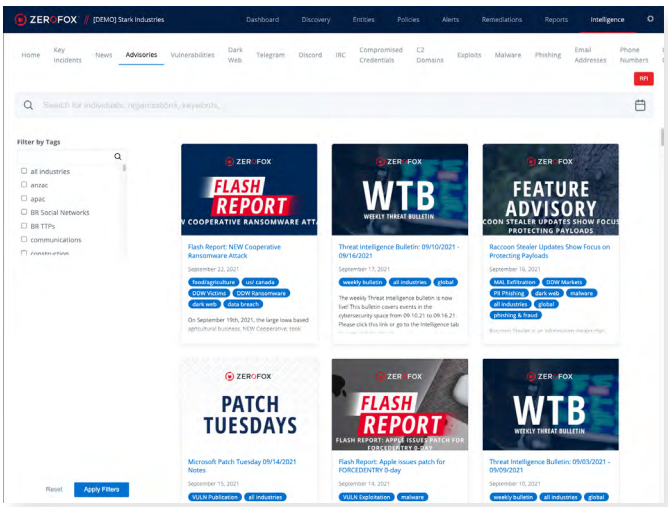
Aborde las amenazas digitales persistentes y acceda a investigaciones y análisis de amenazas en profundidad. Nuestro equipo de expertos analistas proporciona acceso a investigaciones de amenazas personalizadas y a detallados estudios basados en los ataques, casos de uso, solicitudes de investigación nuevas y/o problemas persistentes concretos para su organización.

Anuncios públicos

Las nuevas publicaciones a lo largo de la semana garantizan que su equipo de seguridad esté al día sobre los últimos ciberdelincuentes y las nuevas campañas. Los anuncios incluyen avisos de violaciones de datos, ataques dirigidos, informes de investigaciones y otro material.

Informes sobre inteligencia estratégica

Aproveche las investigaciones y los informes de ciberinteligencia periódicos que ofrecen información sobre las políticas, la planificación y la implementación de seguridad, así como las operaciones en curso. Nuestras investigaciones selectivas facilitan la toma de decisiones más efectivas sobre políticas y cumplimiento, refuerzan la seguridad y mejoran las operaciones de seguridad rutinarias.



MÓDULO DE BÚSQUEDA DE AMENAZAS

El módulo de búsqueda de amenazas de ZeroFox proporciona a los analistas de inteligencia de amenazas acceso ilimitado al completo lago de datos de inteligencia de amenazas desde la plataforma ZeroFox. Disfrute de la posibilidad de buscar en el extenso lago de datos de ZeroFox y recuperar toda la inteligencia de amenazas relacionada con los términos de búsqueda. Puede buscar fácilmente en fuentes de inteligencia y de vulnerabilidades con información procesada y filtrada, y en los IoC asociados para localizar actividad de Command & Control (C2), canales de comunicación furtivos, credenciales comprometidas, etc.

Recursos para defenderse

Más de 200
investigadores y analistas de inteligencia en nuestro equipo global

Más de 50
agentes integrados en la web oscura para participar en mercados clandestinos de ciberdelincuentes

Más de 15
años de experiencia promedio

Más de 30
idiomas

COLECCIÓN DE INTELIGENCIA GLOBAL

ZeroFox proporciona inteligencia sobre amenazas integral "externa al firewall" para las plataformas empresariales digitales de las que depende. Ofrecemos un conjunto de inteligencia automatizada y humana para los recursos protegidos de todas las fuentes de datos: de superficie (OSINT) y de la web profunda y oscura. Esto permite descubrir y responder a las amenazas antes de que el daño esté hecho.

ZeroFox cubre una amplia gama de fuentes de datos, como redes sociales y registros de dominios, correo electrónico, sitios de la web de superficie, profunda y oscura, foros y marketplaces. A medida que surgen nuevas amenazas, nosotros vamos ampliando nuestra cobertura y funcionalidades para satisfacer así las necesidades del mercado.

ZeroFox se ha comprometido a ofrecer transparencia total en cuanto a cobertura de fuentes de datos. La colección de inteligencia global de ZeroFox integra miles de millones de contenidos sociales y digitales, y garantiza que las entidades protegidas se transfieran casi en tiempo real. ZeroFox emplea las API de redes para la ingestión de datos, garantizando el máximo de puntualidad y precisión de los datos.

COBERTURA DE FUENTES DE DATOS

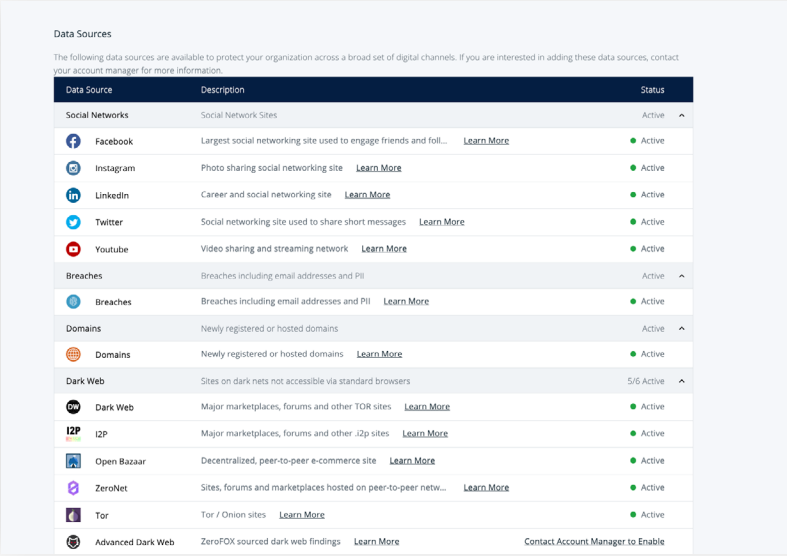
La cobertura de fuentes de datos de ZeroFox* incluye, entre otras:

- Redes sociales regionales e internacionales
- Web oscura y web profunda
- Sitios para pegar compartir código
- Canales de comunicación encubiertos
- Dominios web
- Correo electrónico
- Sitios web de superficie y búsquedas web avanzadas
- Marketplaces web
- Foros, blogs y sitios de revisiones
- Fuentes RSS
- Últimas noticias
- Tiendas de apps móviles
- Vulnerabilidades
- Violaciones de seguridad
- Plataformas de colaboración
- Análisis en la red de IP y nombres de hosts

**Puede acceder a nuestra completa lista de fuentes totalmente actualizada directamente desde la plataforma ZeroFox.*

HERRAMIENTA DE DESCUBRIMIENTO

Con la función de descubrimiento, puede buscar en redes sociales y en la web social (foros y sitios paste), y todo desde una sola consola. Desde la página de descubrimiento, los analistas pueden identificar la presencia de sus organizaciones en las redes sociales, localizar nuevos perfiles que necesitan protección, poner en listas blancas cuentas válidas, buscar cuentas no fiables, identificar perfiles de atacantes, buscar información robada o investigar ataques en proceso de planificación.



INTELIGENCIA DE AMENAZAS GESTIONADA ONWATCH™

Nuestro excelente equipo de expertos en amenazas se ocupa de gestionar a todos y cada uno de los clientes de ZeroFox, lo que ahorra tiempo y esfuerzo a su equipo de seguridad. Ya sea para filtrar alertas en la plataforma ZeroFox, acceder a recursos de inteligencia agrupados o aprovechar la asistencia de un analista totalmente dedicado, puede confiar en nuestra protección personalizada ampliada y en los expertos en inteligencia de amenazas que le ayudarán a garantizar una protección óptima y a satisfacer sus requisitos específicos.

OnWatch™ Alert

Amplíe la visibilidad y la protección digital con ZeroFox OnWatch™ Alert. Nuestro equipo de expertos en amenazas de primera línea del SOC global proporciona servicios gestionados 24x7x365 para revisar, filtrar y escalar los incidentes, así como clasificar las amenazas por prioridades. Garantice la protección de su organización frente a amenazas sociales y digitales, mientras maximiza el valor de la plataforma ZeroFox y recupera más tiempo para dedicar a otras tareas.

OnWatch™ Insight

ZeroFox OnWatch™ Insight amplía el conocimiento de las amenazas mediante expertos e investigaciones en contexto. Disfrute de acceso a grupos de analistas de inteligencia de amenazas, que ofrecen análisis detallados de amenazas, información, informes e inteligencia procesada relevante para su empresa y su sector. Complemente la plataforma ZeroFox basada en inteligencia personal con análisis realizados por expertos humanos para descubrir las amenazas en el contexto de su empresa, sus directivos, sus recursos y sus datos.

OnWatch™ Expert

El servicio ZeroFox OnWatch™ Expert ofrece un analista dedicado que actúa como un miembro esencial de su equipo de operaciones de seguridad. Confíe en un experto analista de inteligencia de seguridad que ofrece asistencia para buscar amenazas en más de 30 idiomas, informes continuos sobre amenazas y resúmenes ejecutivos periódicos. Nuestros analistas acceden al lago de datos de indicadores y datos de amenazas más preciso del mundo, que incluye una información incomparable, procedente de agentes integrados en la web oscura.

Elija el nivel del servicio OnWatch™ adecuado para su organización	OnWatch™ Alert	OnWatch™ Insight	OnWatch™ Expert
Experiencia y servicio gestionado, nivel mundial, 24x7, nivel 1, filtración, validación, direccionamiento y escalada	✓	✓	✓
Soporte para la plataforma y asistencia al cliente, 24x7	✓	✓	✓
Incorporación inicial, instalación y configuración realizadas por un experto, ajuste, optimización de la plataforma y consultas	✓	✓	✓
Diseño del flujo de trabajo para clientes y acceso online, bajo demanda a ZeroFox University	✓	✓	✓
Investigación de solicitudes de información, análisis y consultas de contexto de alertas		✓ 4 respuestas/mes	✓ Sin límite de solicitudes de información
Filtración y análisis de alertas		✓ Limitados	✓ Avanzados
Acceso a grupo de analistas de inteligencia de amenazas		✓	✓
Inteligencia procesada estratégica (amenazas geopolíticas, sectoriales, globales), inteligencia de amenazas semanal e informes de evaluación de amenazas mensuales		✓	✓
Resumen de inteligencia de amenazas diario, resumen ejecutivo de inteligencia de amenazas trimestral y búsqueda de amenazas proactiva			✓
Acceso a analistas de inteligencia de amenazas sénior dedicados (tiempo completo o media jornada)			✓
Soporte en distintos idiomas	Solo en inglés	Solo en inglés	En más de 30 idiomas

INVESTIGACIONES BAJO DEMANDA Y OPERACIONES EN LA WEB OSCURA (DARK OPS)

Consiga acceso a equipos de analistas e investigadores de inteligencia muy especializados, con experiencia en evaluaciones de riesgos e investigaciones de alto nivel. Además, puede contar con la aportación de agentes muy integrados en la web oscura que contactan con los adversarios, clasifican las amenazas y filtran la inteligencia relevante para su caso.

Investigaciones bajo demanda y asistencia para incidentes

Las amenazas contra recursos físicos y digitales van en aumento en cuanto a escala y a nivel de sofisticación. La mayoría de las organizaciones no disponen de las herramientas, el personal ni el tiempo necesarios para afrontar este incremento, sin embargo el éxito de su empresa sigue dependiendo de su capacidad para evaluar y responder con precisión. El servicio de investigación bajo demanda y asistencia para incidentes de ZeroFox proporciona analistas de inteligencia muy cualificados que ofrecen informes muy detallados, análisis técnicos de ciberseguridad, evaluaciones de amenazas, proyectos de investigación y proyectos de análisis a petición, adaptados para su organización.

Consiga análisis en profundidad de sus adversarios, las campañas, los objetivos, actividades de equipo rojo, evaluaciones e informes de la superficie de ataque, según sus solicitudes de información específica (SIR), sus solicitudes de inteligencia prioritarias (PIR) y sus solicitudes de información (RIF).

Investigación e interacción con Dark Ops

Llegue a niveles más profundos del mercado clandestino de la ciberdelincuencia con la inteligencia de amenazas de la web oscura que proporciona ZeroFox. Nuestros analistas trabajan con agentes de la web oscura para investigar e identificar credenciales expuestas, datos de identificación personal, propiedad intelectual, y cuentas de redes sociales y de Active Directory suyas que estén a la venta en la web oscura. Además, nos encargaremos de responder a cualquier solicitud de información concreta que se plantee.

ZeroFox también emplea a agentes de la web oscura muy infiltrados, con conexiones exclusivas con las comunidades *underground*, para ayudarle a recuperar sus recursos, negociar precios y adquirir material comprometido específico. Consiga acceso a los agentes y las investigaciones de Dark Ops en cualquier momento. Hay servicios, informes y evaluaciones disponibles a través de suscripción y bajo demanda.

NEUTRALIZACIÓN Y DISRUPCIÓN

Disrupción de ataques y desmantelamiento de la infraestructura del adversario

DESMANTELAMIENTO COMO SERVICIO

ZeroFox le ahorra el esfuerzo y los costos del proceso manual de localizar y desarticular perfiles maliciosos, y cancelar comentarios peligrosos, actuando en su nombre para empaquetar y reportar directamente al proveedor de la fuente para llevar a cabo la eliminación. ZeroFox ofrece las funciones de desmantelamiento automático más eficaces y más amplias de todos los proveedores de seguridad para una amplia variedad de fuentes de datos, como redes sociales, web, web profunda y oscura o dominios, lo que le ahorra tiempo y recursos.

- Identificación y alertas sobre riesgos: cuando la plataforma identifica riesgos, genera alertas en tiempo real. Con cada alerta, nuestro equipo de expertos analiza y escala el problema, según los datos del riesgo, el contexto y el adversario descubiertos.
- Neutralización y eliminación de amenazas: ZeroFox elimina directamente el contenido, los perfiles y las cuentas que infringen los términos de servicio de las plataformas digitales. Con ZeroFox, todo se lleva a cabo sin que usted tenga que mover ni un dedo.
- Ocultación de comentarios ofensivos: ZeroFox puede identificar y ocultar rápidamente comentarios y publicaciones destinadas a dañar la reputación de su marca o a hacerse pasar por su organización. Cuando se ocultan comentarios y publicaciones en cuentas con un propietario, estos se hacen invisibles para el público, sin avisar a la persona que publicó este contenido ni eliminarlo completamente.
- Bloqueo de perfiles maliciosos: evite que los perfiles maliciosos puedan publicar en páginas propiedad de otros, bloqueando estas cuentas fraudulentas. Al bloquear los perfiles, se impide que los ciberdelincuentes puedan interactuar o comunicarse con la marca y la empresa online.
- Eliminación de contenido perjudicial: ZeroFox le ayuda a borrar comentarios, publicaciones y perfiles que infringen los términos de servicio y amenazan la reputación de la marca en los canales digitales.

Disrupción a escala

>700 Partners de disrupción a nivel mundial, en aumento

>150,000 Promedio de desmantelamientos realizados por trimestre

97 % Tasa promedio de desmantelamientos de killchain

DISRUPCIÓN DEL ADVERSARIO

Vaya más allá de los desmantelamientos definitivos, adoptados de forma reactiva, y lleve a cabo acciones continuas y decisivas para impedir que los adversarios puedan lanzar ataques futuros. ZeroFox correlaciona y aprovecha datos de amenazas recopilados de una gran comunidad de clientes y los comparte con partners proveedores externos para disrumpir y desmantelar con eficacia la infraestructura de ataque completa del ciberdelincuente.

- Detecte y monitoree las señales de aviso de ataque y corte cualquier intento de primer contacto, mediante las siguientes tácticas:
  - Envío de listas de elementos no autorizados (o listas negras) para Google Safe Browsing, VirusTotal, Anti-Phishing Working Group, etc.
  - Presentación automática a las principales empresas de registro, proveedores de hostings, proveedores front end de la nube, etc.
  - Correlación de datos de análisis de DNS y kits de phishing para pivotar en infraestructuras de campaña más grandes.
- Consiga visibilidad de la plataforma sobre acciones de disrupción emprendidas contra un ataque de phishing dirigido a un dominio (como la distribución de indicadores de compromiso a la Red de Disrupción Global), junto con información adicional sobre el estado y el contexto, como el envío de solicitudes de desmantelamiento a hosts, empresas de registro de dominios, etc.

RED DE DISRUPCIÓN GLOBAL (GDN)

La Red de Disrupción Global (Global Disruption Network, GDN) es una red de distribución que facilita la entrega rápida de URL e indicadores maliciosos a proveedores externos, con la posibilidad de neutralizar la actividad maliciosa antes de eliminarla completamente. ZeroFox usa un endpoint con API dedicada para distribuir las URL y los indicadores de compromiso (IoC) maliciosos conocidos a aproximadamente cien de los mayores proveedores digitales del mundo, entre los que se encuentran proveedores de Internet (ISP), CDNS, de hosting, de registro de dominios o de seguridad de endpoints, entre otros.

La disrupción del adversario funciona en tiempo real, lo que agiliza considerablemente la neutralización y bloquea futuros ataques de forma proactiva.

Biblioteca de apps e integraciones

FUENTE DE INTELIGENCIA DE AMENAZAS INTEGRADA

ZeroFox monitorea las conversaciones entre ciberdelincuentes sobre la venta de información personal, concretamente credenciales y tarjetas de crédito comprometidas de la web profunda y oscura a través de una fuente de amenazas conectada a API.

ZEROFOX APP CONNECTOR

ZeroFox App Connector ofrece alertas de la plataforma, inteligencia de amenazas e indicadores de compromiso (IoC), así como integración con otras herramientas de seguridad como Splunk, SIEM, TIP y SOAR. Aproveche las aplicaciones de partners disponibles para optimizar su respuesta a las amenazas externas, gracias a un eficaz enriquecimiento de la inteligencia de amenazas, la orquestación de las alertas y la neutralización de incidentes.

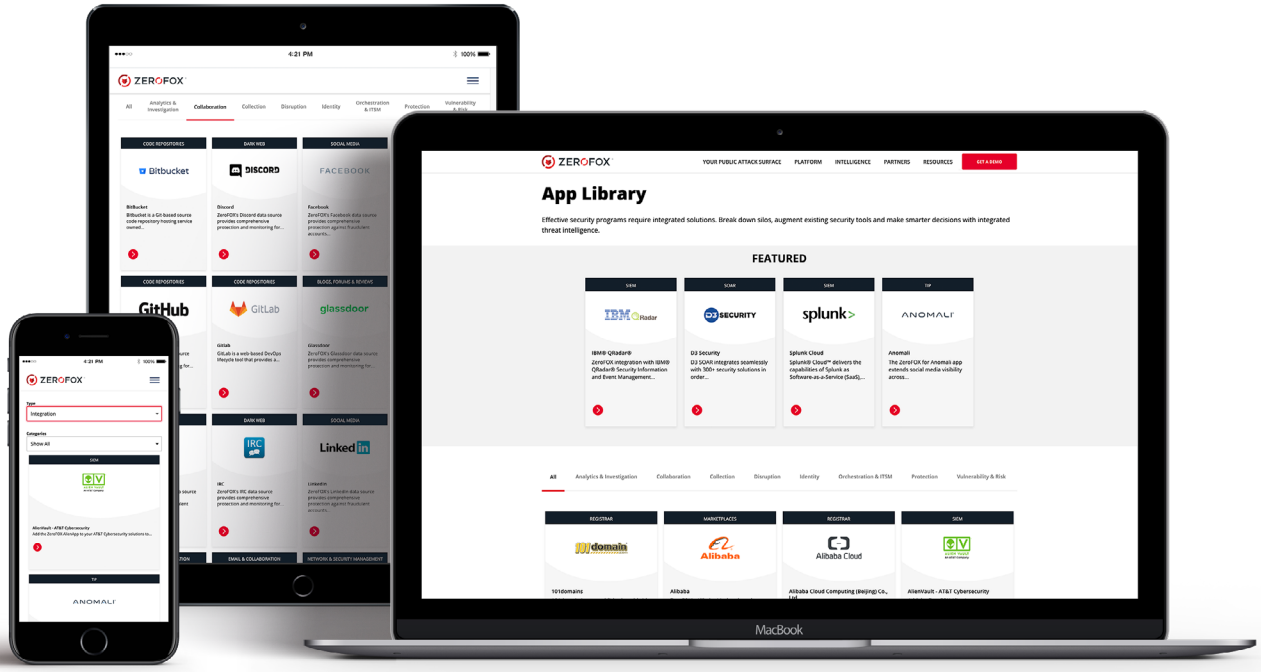
BIBLIOTECA DE APPS DE ZEROFOX

Los programas de seguridad eficaces necesitan soluciones integradas. Conecte a su empresa con ZeroFox para disfrutar de inteligencia de amenazas integrada. Acceda a más de 700 fuentes de datos, apps de disrupción y tecnología, API REST ampliables y conectores preincorporados para las herramientas que ya ha desplegado.

Vea aquí la biblioteca de apps de ZeroFox: **zerofox.com/app-library/**.

La plataforma ZeroFox conecta con:

- SOC existentes (TIP, SOAR, SIEM, infraestructuras, etc.)
- Herramientas de análisis e investigación
- Proveedores de colaboración
- Proveedores de recopilación
- Proveedores de disrupción de amenazas
- Aplicaciones de identidad y de SSO
- Protección
- Herramientas de orquestación e ITSM
- Aplicaciones de protección
- Aplicaciones de vulnerabilidades y riesgos



Funciones de análisis y de la plataforma basadas en inteligencia artificial

ANÁLISIS CON INTELIGENCIA ARTIFICIAL

Reduzca significativamente su exposición a riesgos con análisis basados en IA y reglas personalizadas, diseñadas para eliminar los costos y el tiempo invertido en la búsqueda de amenazas, la neutralización manual y las lagunas de protección. Las funciones de IA de ZeroFox incluyen aprendizaje automático, visión por computadora y comparación facial para detectar amenazas en texto, imágenes y video, no disponibles en las soluciones de seguridad tradicionales. Aproveche el poder de las tecnologías basadas en IA para estar informado de las amenazas críticas, con acceso en la oficina o a través de un dispositivo móvil mediante la app para móviles de ZeroFox.

ALERTAS

Una vez que se han configurado las entidades y se han establecido las políticas, ZeroFox comienza a identificar continuamente las violaciones de seguridad nuevas y a activar las alertas correspondientes. Las alertas masivas se muestran en una tabla que se puede filtrar fácilmente y que permite ordenar las alertas por calificación de riesgo, entidad afectada, tipo de amenaza, fecha/hora, red social y otros muchos criterios. Cada alerta incluye el contenido o perfil ofensivo, los metadatos de la amenaza, la inteligencia del adversario, los registros de alertas y la posibilidad de aplicar medidas para la alerta, como su asignación o envío por correo electrónico, la inclusión del adversario en una lista blanca y la solicitud de eliminación del contenido. Todos estos datos de alertas, así como los metadatos enriquecidos adicionales, están disponibles a través de una API para que las organizaciones las puedan incorporar a su infraestructura de seguridad existente.

FOXSCRIPTS - ANÁLISIS PERSONALIZADOS

FoxScript, una parte de la plataforma ZeroFox, es un lenguaje basado en JavaScript que permite aprovechar las ventajas de los motores de recopilación y análisis de datos de ZeroFox prácticamente en cualquier caso de uso. Esta función de ajuste permite a las organizaciones regular el volumen de sus alertas, garantizar que solo se transmita a los analistas de seguridad la información más crítica y evitar la sobrecarga de datos.

PANEL Y ACCESO

El panel de ZeroFox proporciona un resumen global del estado general de los riesgos digitales y las medidas de mitigación implementadas para la organización. El panel muestra el número total de publicaciones, perfiles, URL e imágenes ingeridas y analizadas, y ofrece una visión global de las alertas más críticas y las entidades más amenazadas. Además, proporciona un resumen de métricas de desmantelamiento y anuncios recientes de los investigadores de ZeroFox. ZeroFox utiliza también el control de acceso basado en roles (o RBAC) para la visibilidad de las páginas, que permite ocultar o mostrar determinadas páginas en función de los usuarios, roles o grupos existentes. Esta funcionalidad ayuda a prevenir numerosos problemas, como la modificación incorrecta de configuraciones importantes de la plataforma por parte de usuarios no autorizados.

REGLAS Y POLÍTICAS

Una vez que las entidades se han configurado, puede determinar, según los casos de uso asociados, qué análisis realizar para cada una de ellas (por ejemplo, una marca tendrá distintos requisitos que un empleado). El motor de reglas de ZeroFox emplea una combinación de técnicas de inteligencia artificial, aprendizaje automático y ciencia de datos para superar las dificultades del ingente volumen de datos ingeridos, por una parte, y la diversidad de riesgos, por otra. Dispone de control total sobre qué políticas activar y qué políticas aplicar a cada entidad. ZeroFox viene de fábrica con cientos de reglas predeterminadas para los problemas más destacados en redes sociales, como los relacionados con enlaces maliciosos, suplantación de cuentas, violencia, contenido ofensivo, cuentas comprometidas, incumplimiento de normativas (PCI, FFIEC, HIPAA, RGPD, etc.), estafas, información de identificación personal (PII) y mucho más.

GENERACIÓN DE INFORMES

Informes de resumen automatizados y rigurosos que incluyen estadísticas clave de la plataforma acerca de la presencia en redes sociales y medios digitales, las principales amenazas identificadas y las soluciones implementadas por la plataforma ZeroFox. Además, ZeroFox proporciona herramientas e informes para exportar datos de la plataforma con el fin de realizar análisis personalizados y utilizarlos en otros sistemas.

Éxito del cliente

LANZAMIENTO E IMPLEMENTACIÓN

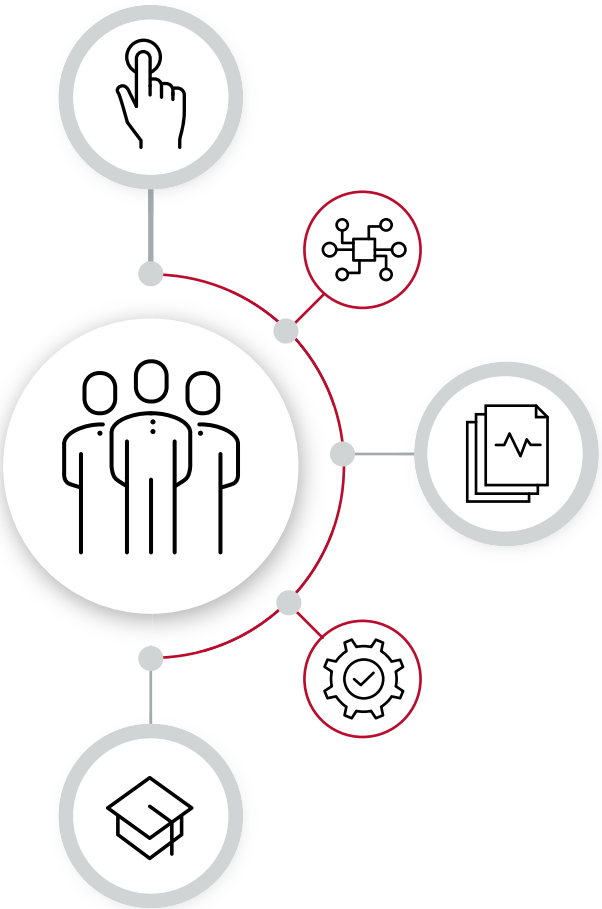
El equipo de expertos en lanzamiento de ZeroFox garantiza que su plataforma esté configurada para el éxito continuo. Con nuestro programa de lanzamiento personalizado tendrá la seguridad de que su protección esté meticulosamente configurada según las necesidades concretas de su organización.

SERVICIOS GESTIONADOS, PROFESIONALES Y TÉCNICOS

ZeroFox ofrece una amplia variedad de servicios flexibles y adaptados para ayudarle a evaluar, analizar y reducir el riesgo digital para su organización. Nuestro equipo de expertos puede ayudarle a crear integraciones, adaptar, optimizar y configurar la plataforma, y mejorar su experiencia general en la plataforma.

ZEROFOX UNIVERSITY

ZeroFox ofrece programas de formación, tanto técnica como de otro tipo, para que usted y su equipo saquen el máximo partido a la inversión en la plataforma ZeroFox. Los usuarios pueden aprovechar esta certificación de nivel profesional para proteger mejor a su organización y para desarrollar su carrera profesional.



Comience con ZeroFox

1 Decida qué es lo importante

Ajuste la plataforma para recopilar los datos que son relevantes para su organización, configurando sus entidades o investigue qué es lo relevante empleando el inmenso y exhaustivo lago de datos de inteligencia de amenazas de ZeroFox.

2 Defina sus políticas

Decida qué reglas y políticas listas para usar se van a activar para lo que desea proteger. Además, ZeroFox le ofrece acceso total para escribir sus propias reglas de FoxScript personalizadas, según los casos de uso específicos de la organización.

3 Amplíe su equipo

Maximice los recursos de su equipo sumando un equipo de servicio de inteligencia de amenazas global de élite para investigaciones, estudios, análisis, informes, interacciones con dark ops, etc.

4 Reciba alertas sobre riesgos

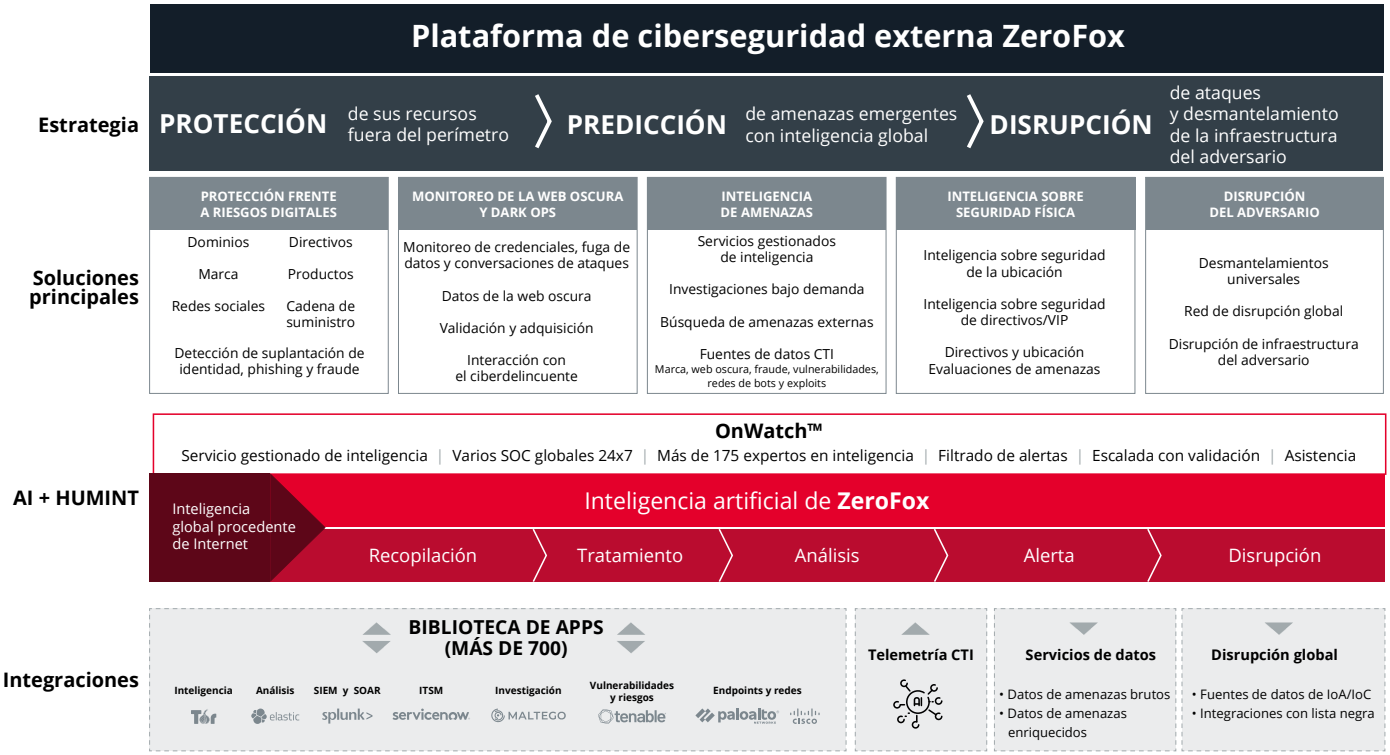
Reciba automáticamente alertas en tiempo real cuando la plataforma identifique los riesgos. Cada alerta incluye inteligencia de amenazas en contexto, registros de alertas, información del autor y medidas para la neutralización.

5 Eliminación de contenido malicioso y disrupción de ataques

Presente solicitudes de desmantelamiento y controle su evolución desde dentro de la plataforma. ZeroFox elimina el contenido peligroso y automatiza la distribución de las URL e indicadores maliciosos a proveedores externos para facilitar el bloqueo y la desarticulación de la infraestructura del atacante.

6 Integre los datos en su entorno

Aproveche una de las cientos de integraciones de ZeroFox o bien utilice las API RESTful de ZeroFox para incorporar los datos de las alertas en su entorno de seguridad y procesar las medidas de neutralización por la plataforma.



La plataforma ZeroFox proporciona ciberseguridad externa integral para proteger sus recursos más allá del perímetro. Predicción eficaz de amenazas, disrupción de ataques y desmantelamiento de la infraestructura del atacante.

ACERCA DE ZEROFOX

ZeroFox, líder en protección e inteligencia de amenazas externas, proporciona a las empresas protección, inteligencia y medidas para frustrar las amenazas contra marcas, individuos, recursos y datos en toda la superficie de ataque pública. Con cobertura completa de la web de superficie, la web profunda y la web oscura, y con un motor de análisis basado en inteligencia artificial y tecnología de Intel, la plataforma ZeroFox identifica e impide los ataques de phishing dirigidos, el robo de credenciales, la filtración de datos, el secuestro de marcas, las amenazas a directivos y ubicaciones, etc. La tecnología patentada de la plataforma ZeroFox procesa y protege diariamente millones de publicaciones, mensajes y cuentas en la superficie de ataque pública, que incluye la web de superficie, la web profunda y la web oscura, los dominios, las redes sociales, las tiendas de aplicaciones móviles, el correo electrónico en la nube, etc.